Digital Rights Management: A Contrarian's View

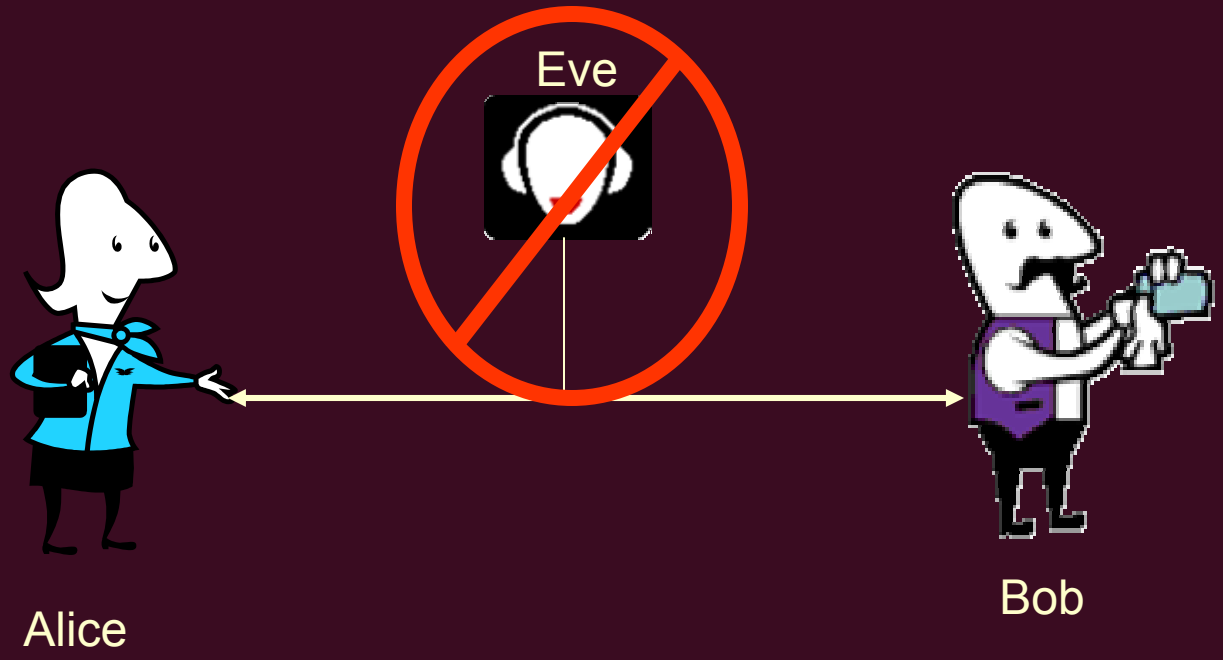
Drew Dean
SRI International
Computer Science Laboratory

Reminder

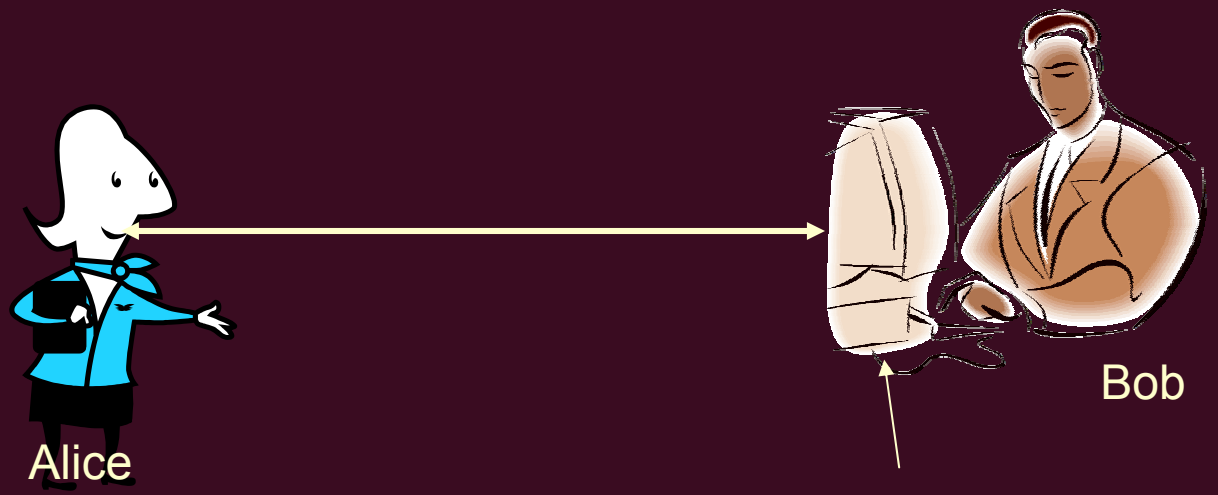
- I make my living courtesy of IP law.

Crypto for Confidentiality

Standard Model of Cryptography
We think we know how to do this



The DRM Problem

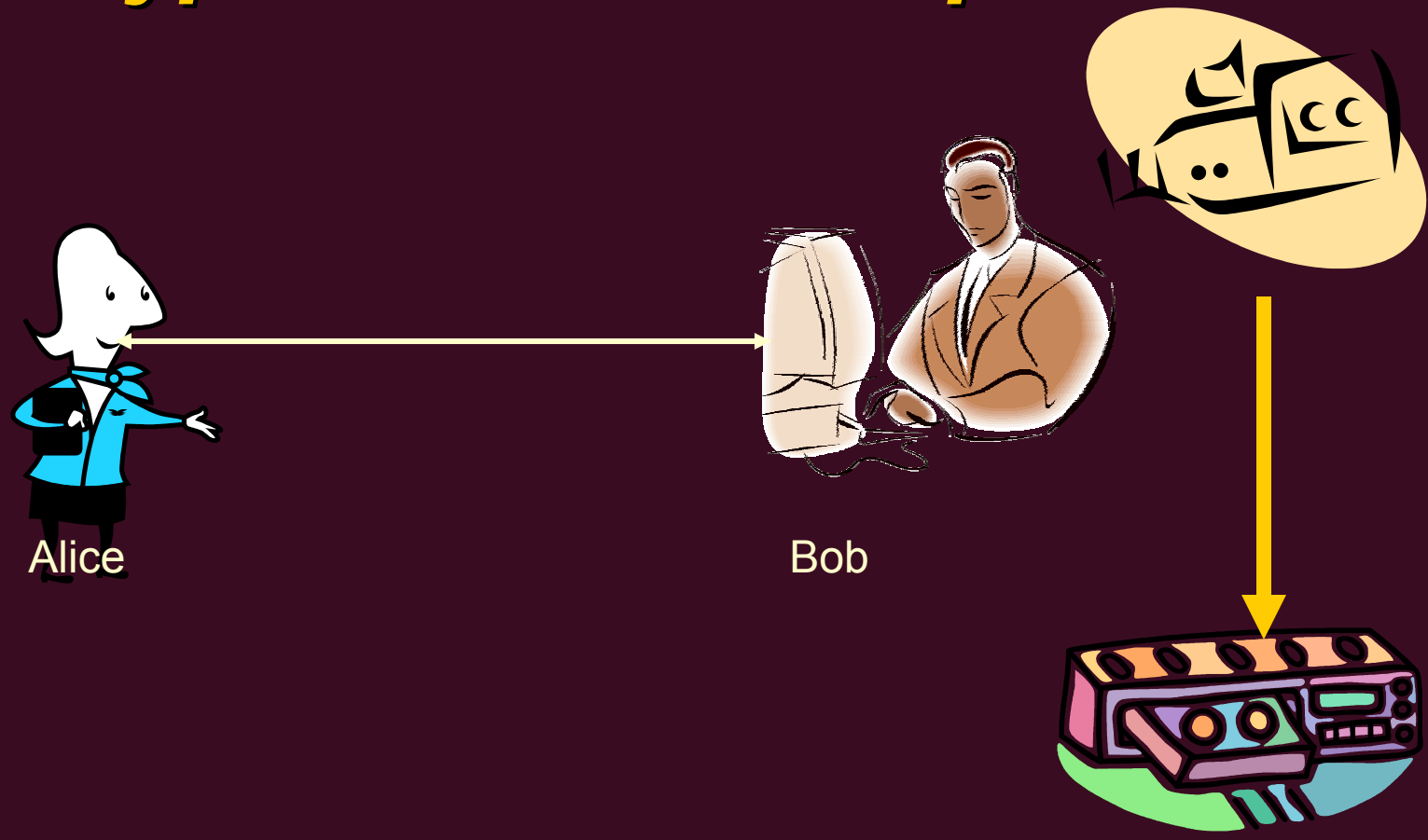


Questions for lawyers

- What does it mean to “own” something that I’m not allowed to understand how it works?
- Am I responsible for what my computer does without my knowledge?

The DRM Problem

Crypto does not help!



Closed Design

- All DRM systems so far have been designed in secret
- Recent (post-1980) cryptographic solutions have been designed in public
  - E.g., the AES competition to replace DES
- The history of closed designs' security is riddled with failures
- Only the NSA is large enough to do meaningful internal review

Subtle cryptographic errors

- It can take nearly forever to find problems in cryptographic protocols
- Needham-Schroeder Public Key
  - 3 messages
  - 18 years to find the problem!
  - While being a standard example in the literature
- DRM faces an even harder problem: Adversary has many more attacks
    - Power analysis
    - Timing analysis
    - Fault injection

Security & Cryptology as a Game

- New algorithms, modes of operation, protocols, etc. proposed all the time
  - You need serious credentials before you'll be taken seriously
- Many broken in time for next year's conference
- Repeat

Security & Cryptology as a Game

- When things are open, this game works well
- Harder, but possible, in a closed world
  - E.g., DRM systems
- Impossible with DMCA, EU Copyright Directive, etc.

Security & Cryptology as a Game

- Assertion: We don't know how to solve the DRM problem today.
- We can't proceed to play the usual research game
- Hence, we will *never* solve the DRM problem

Other Relevant Technologies

- Watermarking
- Code obfuscation

Watermarks

- Robust Watermarks
  - Meant to withstand transformations that leave original recognizable
    - Images: scaling, cropping, rotation, etc.
    - Sound: transposition, noise, time dilation, etc.
      - Lossy compression
- Fragile Watermarks
  - Any change is detectable
- Both: meant to be imperceptible by people

Uses of Robust Watermarks

- Usage tracking
- Metadata storage
- DRM policy enforcement

Uses of Fragile Watermarks

- Integrity protection of originals
- Detecting lossy compression
- This appears to be solvable

SDMI Challenge

- September 2000, 3 weeks
- No documentation
- 4 “robust” watermark technologies
- Devastating results:
  - Craver, Wu, Liu, Stubblefield, Swartzlander, Wallach, Dean, Felten, “Reading Between the Lines: Lessons Learned From the SDMI Challenge,” USENIX Security Symposium, 2001.
  - Stern and Boeuf, “An analysis of one of the SDMI candidates,” Information Hiding Workshop, 2001

Code Obfuscation

- Software is malleable
- Tamper-resistant hardware is rare and expensive
- Can we obfuscate software for better security?

Code Obfuscation

- In a completely general way, no
  - Barak, et al., On the (Im)Possibility of Obfuscating Programs, CRYPTO 2001
- Cloakware has tried hiding a key in a DES implementation
  - Jacob, Boneh, Felten, “Attacking an obfuscated cipher by injecting faults,” ACM DRM workshop, 2002
- No good, uniform definitions of the problem

DRM: Technical Summary

- Crypto doesn’t just solve the problem

DRM Paradox

- Most security needed for low unit cost, mass market items
  - That's where the big money is
  - High unit cost items (e.g. market research reports) have different business models/needs

The Real Reason DRM will fail

- Technical problems will persist, but …
- Consumer will pocket veto technologies that fail offer consumers good value propositions by doing nothing
  - An exceedingly simple process for the consumer: keep wallet firmly in pocket

Sony Music Clip

- Critics:
  - “Worse, it treats every user like a potential criminal, and tries to impose new controls on music people paid for years ago. So I actually found it insulting, as well.”
  - “Sony seems so concerned about copyright that it has made getting music onto the Clip a pain…. Can you imagine Sony product managers sitting around a conference room, planning to make a product more frustrating to use?”

Sony Music Clip

- Critics:
  - “Worse, it treats every user like a potential criminal, and tries to impose new controls on music people paid for years ago. So I actually found it insulting, as well.” – Walter Mossberg, The Wall Street Journal, March 2, 2000
  - “Sony seems so concerned about copyright that it has made getting music onto the Clip a pain…. Can you imagine Sony product managers sitting around a conference room, planning to make a product more frustrating to use?” – Stewart Alsop, Fortune, February 21, 2000

Conclusions

- Technical measures for DRM have a bad track record
- Technical solutions to legal problems are a bad idea
- Legal solutions to technical problems are a bad idea